Enhancing Security in Mobile IPv6

Hero Modares, Amirhossein Moravejosharieh, Rosli Bin Salleh, and Jaime Lloret

In the Mobile IPv6 (MIPv6) protocol, a mobile node (MN) is a mobile device with a permanent home address (HoA) on its home link. The MN will acquire a care-of address (CoA) when it roams into a foreign link. It then sends a binding update (BU) message to the home agent (HA) and the correspondent node (CN) to inform them of its current CoA so that future data packets destined for its HoA will be forwarded to the CoA. The BU message, however, is vulnerable to different types of security attacks, such as the man-in-the-middle attack, the session hijacking attack, and the denial-of-service attack. The current security protocols in MIPv6 are not able to effectively protect the BU message against these attacks. The private-key-based BU (PKBU) protocol is proposed in this research to overcome the shortcomings of some existing MIPv6 protocols. PKBU incorporates a method to assert the address ownership of the MN, thus allowing the CN to validate that the MN is not a malicious node. The results obtained show that it addresses the security requirements while being able to check the address ownership of the MN. PKBU also incorporates a method to verify the reachability of the MN.

Keywords: Mobile IPv6, binding update, security threats in MIPv6, return routability, cryptographically generated addresses, private key.

Manuscript received Feb. 22, 2013; revised July 02, 2013; accepted July 26, 2013.

This work was supported in part by University of Malaya, Kuala Lumpur, Malaysia under UMRG Grant (RG080/11ICT).

Hero Modares (phone: +60 17 666 4612, Hero.Modares@gmail.com) and Rosli Bin Salleh (rosli_salleh@um.edu.my) are with the Department of Computer System and Technology, University of Malaya, Kuala Lumpur, Malaysia.

Amirhossein Moravejosharieh (amir.moravejosharieh@pg.canterbury.ac.nz) is with the Department of Computer Science and Software Engineering, University of Canterbury, Christchurch, New Zealand.

Jaime Lloret (jlloret@dcom.upv.es) is with the Department of Communications, Polytechnic University of Valencia, Camino de Vera s/n, Valencia, Spain.

I. Introduction

An IP mobility protocol is designed to allow a mobile node (MN) or a device to move from one network to another during communication with the network even though the MN's point of attachment to the network has physically changed [1]. When a mobile device is disconnected from the present attachment point and gets reconnected to another network, portability is achieved. The IP-layer mobility protocol developed for the IPv6 Internet called the Mobile IP version 6 or MIPv6 [2]-[4], contains three entities: the MN, home agent (HA) and the correspondent node (CN), which is the peer that communicates with the MN. The MN is a mobile device with a permanent home address (HoA) on its home link. When it roams into a foreign link, the MN will require one or more care-of addresses (CoAs). The MN must register one of its current CoAs with the HA if it wants to receive data packets destined for its HoA when it is not in its home link. Therefore, when the MN is located away from home, the packets destined for the MN's HoA will be intercepted by the HA before they are forwarded to the CoA registered by the MN. The MN will run the home registration process to register one of its current CoAs with the HA. A binding update (BU) message is sent to the HA by the MN, thus initializing the home registration process. The BU message contains the HoA and CoA of the MN, which is stored by the HA in the binding cache (BC). By using this binding method, the HA can intercept the message destined for the HoA and forward it to the bonded CoA [5], [6]. The BUs need to be protected to ensure that MIPv6 runs smoothly and without disruption. Basically, there are two issues in the network that need to be addressed: security and privacy [7], [8]. When a BU message is not authenticated, it becomes vulnerable to different types of malicious attacks [9]-[11]. This paper proposes a lightweight protocol with strong security features to protect the BU messages. This protocol is proposed

in view of the weak security features found in existing and earlier protocols. The main contribution of the paper is a new method of securing the BU framework using the IPv6 address format for communications between the MN and the CN. The information gathered for this paper is based on the studies pertaining to the security threats to the BU message in MIPv6. The new method we propose should be able to deal with the different possible attacks on the MN and the CN, which include the false BU (FBU), man-in-the-middle (MITM), and denial-of-service (DOS) attacks.

The remainder of this paper is organized as follows. Section II presents the background of the security threats against the MIPv6. An evaluation of the related security standard for BUs is given in section III. The private-key-based BU (PKBU) protocol is proposed and analyzed in section IV and section V, respectively. Section VI presents a comparison between the proposed protocol and existing protocols. Finally, section VII concludes the paper.

II. Security Threats in MIPv6

The MIPv6 was designed to mobilize the feature of the IPv6 to make communication when using mobile devices. The IPv6, has had security vulnerabilities that include weak BU authentication and authorization. BU is responsible for redirecting data traffic among the various nodes in a network, and its role can be adversely affected due to security vulnerabilities, discussed below.

1. Stealing Traffic

An MN's HoA may be known to anyone and can be stored in the DNS. However, if an "intruder" has knowledge of the address, he can "steal" it to redirect traffic to himself by sending an FBU to the CN (Fig. 1). In such a situation, the data traffic that was originally meant for the MN could be stolen by the intruder or the intruder could hijack the MN's connection to a CN, which could then act as the MN in the connection. All the while, the intruder is not even on the MN and the CN path [12].

2. Man-in-the-Middle Attack

If an intruder is on a two-node communication line, he is performing an MITM attack, which could disrupt communication, such as by altering the packet contents. This can produce an unexpected outcome and definitely not the outcome originally intended by the real packet sender. An intruder could also modify the BU content during a data flow between the MN and the CN. This would indicate an attack or that the current connection between the MN and the CN has been hijacked (Fig. 2) [12].

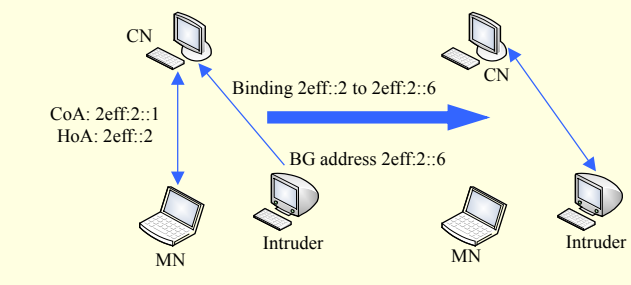

Fig. 1. Stealing traffic (intruder).

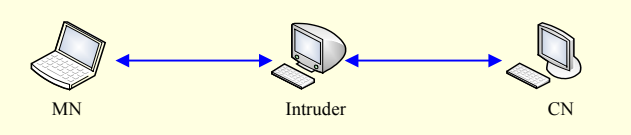

Fig. 2. MITM attack.

3. Denial-of-Service Attack

In a DoS attack, a valid node is denied service, and this can occur in many ways, regardless of whether MIPv6 is used or not. For example, an attacker sends several fake requests to a server to effect a connection, and this will keep the server occupied to the extent that it does not respond to requests from legitimate nodes.

Another kind of DoS attack involves saturating the CN's memory (normally meant for storing BC entries) with lots of fake BUs to fake the HoAs. When the CN's memory becomes full, it cannot process additional messages coming from the real nodes. Similarly, a DoS attack can work against an HA, whereby the attacker disrupts or controls a router on the path between the MN and the CN or the HA. For example, the attacker could refuse service to the MN's packet by dropping it. This sort of attack is not usual for MIPv6, and, in fact, it cannot be prevented, but it can be very difficult, or impossible, for an attacker to compromise the router [12].

III. Related Secure Binding Update Protocols

There are several methods of communication between the MN and the CN in mobile IP. All data traffic between the MN and the CN will be routed by the HA using the standard IPv6 routing mechanism without any special procedures whenever the MN is on its home link [13]. However, when the MN is at a foreign link, there are three possible communication modes:

1. bidirectional tunneling;
2. triangle routing;

ETRI Journal, Volume 36, Number 1, February 2014
http://dx.doi.org/10.4218/etrij.14.0113.0177

3. route optimization (RO).

In the bidirectional tunneling mode, all data traffic is routed indirectly to the MN's home link. This means that all of the CN's packets destined to the MN are routed to the home link of the MN and are intercepted by the HA before they are forwarded to the MN's CoA via a tunnel. Similarly, packets sent from the MN to the CN are tunneled to the HA ("reverse tunneled"). The packets will then be routed back normally to the CN from the home link. Usually, the IPv6 encapsulation method [14] is used to perform the tunneling between the HAs and the MNs. However, these tunnels must be secure, thus, the IPSec [10] tunnels are used. Figure 3 shows the bidirectional tunneling mode.

In the triangle routing mode, an MN is able to send packets directly to the CNs. Figure 4 shows how the MN is able to deliver packets directly to the CN. Meanwhile, the CN delivers packets to the MN's HoA and the HA routes it to the MN. The weakness in this type of routing, when compared to the use of the direct path, is that the packet travels a longer path from the CN to the MN, thus making it less efficient or less optimal [15]. RO is a standard practice in Mobile IPv6 to eliminate inefficient triangle routing and to route packets between the MN and the CN using the shortest possible path [16]-[18].

In the RO mode, the CNs deal directly with the MNs because they are allowed to skip the HA router. This method is shown in Fig. 5. The MN must register its current location with the CN. In this way, a BC will be created by the CN and the binding information between the MN's HoA and the CoA will be stored. As such, all packets to the MN from the CN will be sent to its CoA instead of the HoA. On the other hand, the HA holds the current addresses of the MNs and will send packets to the MNs whenever a CN does not know the address and send it to the HA. However, the speed of delivery increases if the HA is bypassed with the use of the BU RO method. In the RO mode, a presumably shorter path is used between the MN and the CN so that the traffic level at the HA as well as the home link is minimized [17].

However, the security of RO that deals with the BUs is still a major concern because attackers can use the BU to launch malicious attacks, such as MITM, FBU, DoS, and so on. A few solutions have been proposed to make RO secure. One of the proposed solutions is the use of the return routability (RR) security protocol based on RFC 3775 adopted by the Internet Engineering Task Force.

Presently, the RR method has yet to provide enough security for corresponding registration. This method also incurs large signaling overhead, and this has caused delays in registration because it needs six BU messages for every single connection. These six messages must be exchanged between the MN and the CN to complete a single connection, thus making the procedure quite inefficient. In the RR method, the reachability of the MN is examined on the HoA side and on the CoA side. During the RR process, two secret keys are generated as plain text by the CN and sent to the MN's CoA and its HoA. These two keys will be used by the MN and the CN to create a session key for security during the signaling process that follows. Unfortunately, these keys can be stolen by an attacker to generate the session key and use it to impersonate the MN. As a result, the number of attackers is reduced from any nodes in the Internet to only nodes that are between the CN and the MN on the home link route [19]. Other protocols have been proposed to overcome the limitations of the RR protocol in protecting the BUs from attacks that occur during the communication between the MN and the CN. These protocols

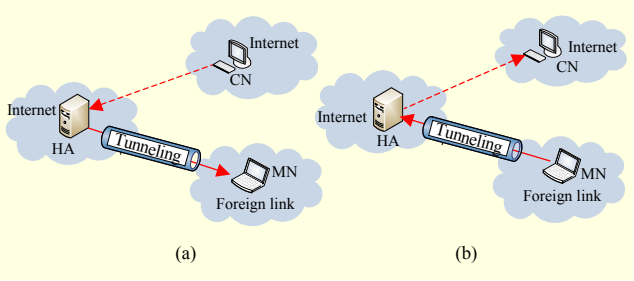

Fig. 3. Bidirectional tunneling: (a) traffic from CN to MN; (b) traffic from MN to CN.

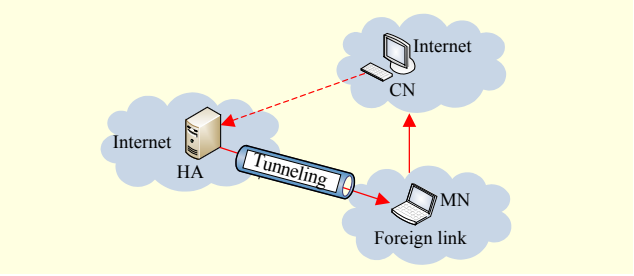

Fig. 4. Triangle routing.

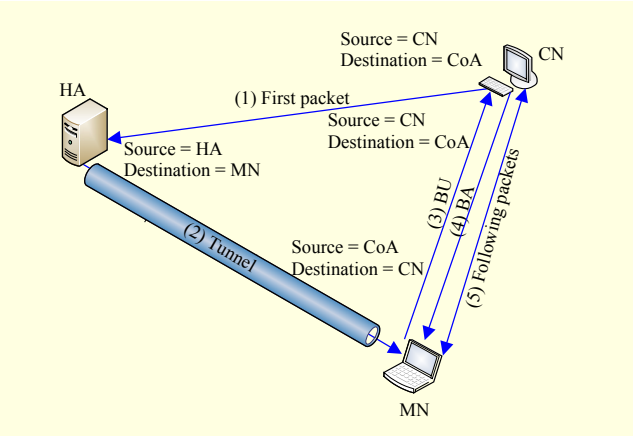

Fig. 5. RO mode.

Table 1. Comparison of INF-less protocols [30].

Protocol	Problem
EBU [21]	Vulnerable to similar on-path attacks as RR.
UDHBU [22]	Vulnerable to DoS, MITM, false BU attacks; attacker is able to intercept the DH public values and sends its own DH public values.
RR [2], [24]	Does not validate IPv6 address ownership; high registration delay; signaling overhead; vulnerable to MITM attack.
OMIPv6 [25]	Attacker is able to intercept DH public values; vulnerable to MITM, FBU attacks.
CGA-OMIPv6 [26]	Anyone can create valid address from valid public key; vulnerable to DoS attack as it cannot authenticate claimed CoA.
ERO-MIPv6 [27]	Has same advantages and disadvantage as CGA-OMIPv6 protocol; involves increased complexity for implementing credit-based authorization technique at CN.
CAM [28]	Open to MN flooding attacks because it is unable to verify authenticity of CoA; it has same weaknesses as CGA-based technique.
PBK [29]	Vulnerable to DoS and MITM attacks.

include cryptographically generated address (CGA) [20], early BU (EBU) [21], unauthenticated Diffie-Hellman BU (UDHBU) [22], certificate-based BU (CBU) [23], RR [24], optimized MIPv6 (OMIPv6) [25], CGA-OMIPv6 [26], enhanced RO for MIPv6 (ERO-MIPv6) [27], child-proof authentication (CAM) [28], and purpose-built key (PBK) [29]. We can divide these protocols into two categories: infrastructure-less (INF-less) and infrastructure-based (INF-based) [30]. INF-less protocols are for general usage on the Internet and widely used all over the world. Using these protocols, the MNs and the CNs belong to their own unique administrative domains. Authentication is allowed between the MNs and the CNs without the need for any security infrastructure. On the other hand, the INF-based protocols generally require some security infrastructure to be in place to provide protection throughout the correspondent registration. This type of protocol provides assurance to the CN that the MN's HoA is valid and correct, which means that the MN's HoA is related to the secret key or the public key of the private/public pair. Our work is based on the protocols of the INF-less category because they offer better security than the INF-based solutions. Table 1 presents a comparison of the studies carried out on the INF-less protocols, along with the weaknesses of each protocol.

IV. Proposed Protocol Schema

The security vulnerabilities of the Mobile IP BUs must be identified to formulate a solution. These weaknesses were discussed in section II. The main cause of these security problems is that attackers are able to steal information regarding the location of the nodes. This is a serious security breach because the address must be presented to transmit the location data. The solution to this problem is to encrypt the data. To do this, however, a secret key has to be exchanged and this process involves the sender and the recipient knowing each other's addresses, and this does not provide a solution. One possible solution is to use a third party as an intermediary to provide authentication and key establishment. This allows the location of the communicating nodes to be kept secret until the nodes have been verified. By centralizing all the information to a third party, the amount of manual configuration will also be minimized. However, there are several weaknesses to this method:

- The centralized source of information is vulnerable by nature, and this is a big disadvantage;
- Constant maintenance is necessary to ensure that the directory is updated;
- All information regarding the nodes is available to the attackers if they were successful in the assault of the third-party directory.

Considering these weaknesses, it is more logical for our proposed solution to be based on the INF-less algorithms. To ensure that the transmission of BU data is more secure, we choose asymmetric cryptography over symmetric cryptography for data encryption because the former has better security features; for example, it provides digital signatures that can be used for user data authentication. We also use a lightweight algorithm, such as the elliptic curve, because it is better at processing data encrypted using the asymmetric cryptography technique. The aim of our proposed solution is to strengthen the security of the BUs. In this context, the following security requirements must be considered in the development of the proposed protocol:

- Verify authenticity of the claimed HoA to assure the CN that the BUs request comes from an entity that actually owns the HoA;
- Verify authenticity of the claimed CoA to assure the CN that the entity that sends the binding request is actually located at the CoA;
- Detect any unauthorized modification of the BU message to protect the integrity of the binding request;
- Ensure that the BUs are protected against FBU, MITM, DoS, and return-to-home spoofing attacks;
- Ensure that the number and length of the messages sent/received at the MN are kept to a minimum.

The functions of the proposed protocol have reduced the need for third-party nodes. This means that all vulnerabilities,

directory upkeep, and central authority attacks can be avoided. Hashes would be included in the BU protocol as part of data integrity checks. A new technique will be introduced to bind the address with the user's private and public keys. A method to verify the authenticity of the location will be proposed to ensure that a node is in the location it claims to be. A suitable complementary solution can be achieved with the combination of a cryptographic system, digital signature; hash function, and IP address creation based on the private key and the public key of the user.

In designing the PKBU, the following measures are taken to fulfill the requirements stated above.

Measure 1: The MN and the CN use the PKBU protocol as specified in section V. The PKBU is used by the MN to register a new CoA whenever it roams away from its original home link. This protocol allows the CN to verify that the CoA belongs to the MN, and it also allows the HA to participate in the correspondent registration. This is done by sending the packet from the MN to the CN. The MN will then be verified by the CN based on these details.

Measure 2: The use of the PKBU protocol will verify that the addresses of the users actually belong to them and are not spoofed addresses. Also, to prevent spoofing, PKBU authenticates the location of the communicating devices and ensures that the IP address is correct. The CN receives a hash value of the authentication data from the MN through the HoA. The data, stored as a hash value by the HA, will be unreadable to attackers who try to intercept it during transmission. The ciphered text will be transmitted by the MN to the CN using the signed private key of the MN. This encrypted and authenticated data is sent from the MN to CN using the MN's private key. The CN can be verified using the MN's public key and decipher the text using that key. The CN then calculates the hash value of the text; if they match, then the authentication process is successful.

Measure 3: By using the PKBU, the centralized authority will be removed and a decentralized authentication system is used instead. The HA, maintained and managed by the Internet service provider, stores the security data of the MN, such as its HoA and CoA. Without any single point of attack, the security infrastructure is secure and safe for the authentication process.

1. Protocol Overview

The proposed PKBU protocol relies heavily on assistance from the MN home link. It needs the home link to enable the CN to verify the authenticity of the MN's HoA and CoA ownership. The MN's HA will confirm to the CN that the MN is the correct owner of the HoA and is connected via the CoA.

A 128-bit IPv6 address is used in PKBU with a 64-bit subnet prefix and a 64-bit identifier. The PKBU uses the interface identifier to provide a strong cryptographic binding between the MN and the CN. It allows the MN to have its own private key and public key. The public key infrastructure (PKI) is no longer needed with this binding ownership of the MN HoA, as the 128-bit IPv6 address hash that is sent provides the proof of the HoA. This can be done in two different ways. Initially, the MN would retrieve its private and public key pair. The user's ID is used to obtain the node's private and public key pairs. In our proposed protocol the node's media access control address is used as the user ID.

In the trust method, the responsibility of ensuring the binding correctness of the MN and its HoA to the CN falls on the MN. Therefore, the CN must be assured by the MN of the following:

1. The HoA ownership belongs to the MN;
2. The MN is the actual BU request.

In the PKBU protocol, the CoA of the MN is certified using the secure interface ID. It is based on the MN's private key with a valid subnet prefix. It should be noted that this method is only used to determine that the HoA belongs to the MN. It does not suggest that the MN also owns the CoA. Once the HoA ownership has been verified, only then will the MN sign the encrypted CoA using the public key of the CN with the HoA using its private key. Doing this proves the correctness of the HoA and CoA binding to the CN. The CN will, in turn, verify the owner of the CoA and HoA by checking the signature of the MN. It will compare the signature with the HoA hash value and the hash value received from the HA.

Figure 6 shows the three phases involved in the exchange of messages between the nodes in the PKBU protocol. Phase 1 consists of three steps in our proposed method to assert the ownership of the MN's IP address. In Phase 2, PKBU checks the reachability of the MN. Phase 3 consists of four steps pertaining to the validation process. It is important to note that the MN assures the ownership and reachability of both HoA and CoA to the CN using the validation process.

Phase 1. This phase consists of the three steps involved in generating the MN's private and public keys and creating the MN's interface ID.

Step 1: Create private key. In this step, the MN creates its own private key, which can be acquired depending on the user ID (Fig. 7). The private key is a number based on the user ID hash value and a random number, meaning that it cannot be predicted, and, thus, it is secure. To obtain the private key, hash function Hash (User ID) * i is used, where "i" is a random integer in the range [1, n–1]. If the private key of the user's MN is an integer, MN_{PRK}, then

$$MN_{PRK} = \text{Hash (User ID)} * i. \quad (1)$$

Step 2: Create public key. In this step, the MN creates its

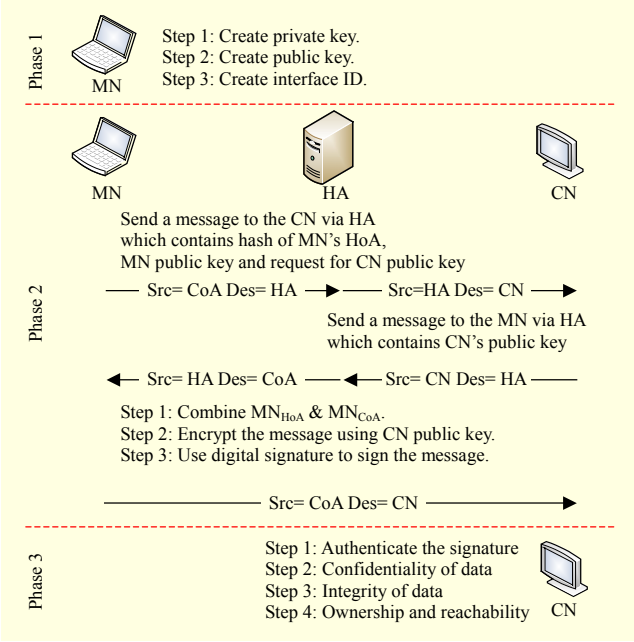

Fig. 6. Phases of PKBU.

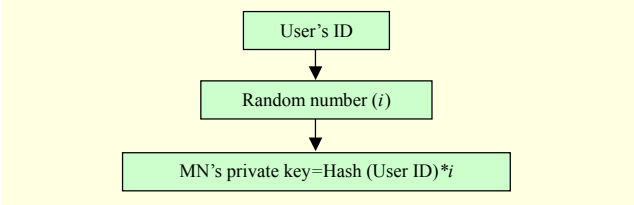

Fig. 7. Generating private key in PKBU.

public key using the elliptic curve cryptography (ECC) method. The sender uses the receiver's public key to encrypt the message, then signs it using its private key. The receiver then decrypts the ciphered message using its own private key and uses the sender's public key for verification. Thus, one of ECC's advantages over other asymmetric algorithms is that it offers the same level of security but uses smaller size keys. ECC implementation is also much more efficient, as it consumes less power and computes faster. Less memory and bandwidth are required due to the shorter bit length of the key [31]. Such attributes are particularly attractive in security applications with restricted computation of power and integrated circuit space [32]. ECC is a public key cryptography, and every user or device involved in the communication process would normally have a pair of keys (public key and private key) as well as a set of operations associated with the keys for performing cryptographic operations. Therefore, only the legitimate or valid user knows the private key, while all other users in the communication process would only receive the public key. ECC mathematical processes are characterized by the elliptic curve $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$.

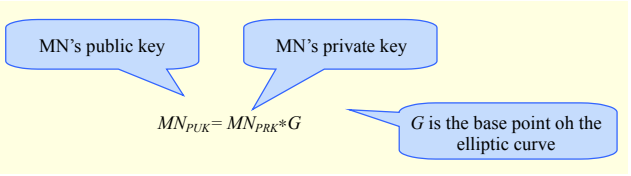

Fig. 8. Creating public key for PKBU.

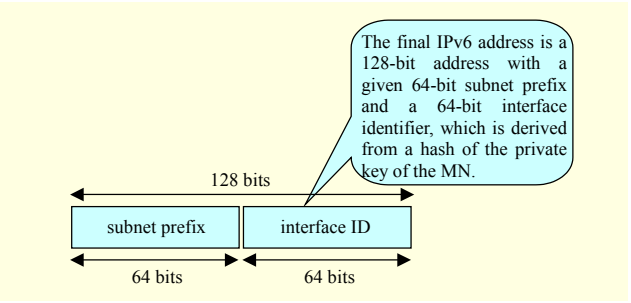

Fig. 9. 128-bit IP address (subnet prefix, interface ID).

Each "a" and "b" value produces a different elliptic curve, and all points (x, y) that satisfy the above equation, including a point at infinity, lie on the elliptic curve. The public key is a point on the curve obtained by multiplying the private key with the generator point G in the curve. The ECC parameters are $T = \{a, b, G, n\}$, where a and b are parameters of the elliptic curve E: $y^2 = x^3 + ax + b$, "G" is the base point on the curve and "n" is the elliptic curve order. If the private key of MN is an integer MN_{PRK}, then MN's public key (MN_{PUK}) is "$MN_{PRK}*G$," which is also a point on E. Hence, a public key is a point on the curve generated from a private key. Thus, the MN has its own public and private keys, which will be used to check the ownership of the IP address of the MN (Fig. 8).

Step 3: Create interface ID. In this step, the MN creates the final 128-bit IPv6 address. The IPv6 has a 128-bit address, together with a given 64-bit subnet prefix and a 64-bit interface identifier, derived from an MN's private key hash value. This new method creates a solid cryptographic binding between the MN's interface identifier and the MN owning the private key (Fig. 9). The binding proves the MN ownership of the HoA, without the need to use a PKI.

Phase 2. The MN sends the CoA to the HA via IPSec. Every time an MN enters a new network, it will be configured with a new CoA. The MN then must register its new CoA and other operations with its HA before the new CoA can be used [24].

Step 1: Send Message 1. Message 1 will be sent through the HA together with all the requirements for routing optimization to the CN. These include the MN's HoA hash value and the public key of the MN obtained in Phase 1. The MN will also request access to the CN's public key ($ReqCN_{PUK}$). The message contains the CN's address to indicate the first

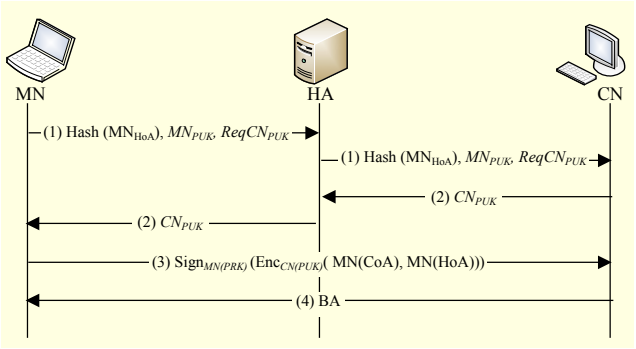

Fig. 10. Proposed protocol.

destination of the message (Fig. 10).

- **Source: MN(CoA) → Destination: HA** Hash (MN(HoA)), MN_{PUK}, $ReqCN_{PUK}$ (it is sent to the HA via a preestablished secure tunnel of IPv6).
- **Source: HA → Destination: CN** Hash (MN(HoA)), MN_{PUK}, $ReqCN_{PUK}$.

Step 2: Send Message 2. In Message 2, the BU message preparation is completed and the CN sends its own public key to the MN through the HA, and the CN stores the hash value of the MN's HoA and MN's public key.

- **Source: CN→ Destination: HA** (CN_{PUK}) (MN receives CN_{PUK} from the HA and prepares Message 3, which has the BU).
- **Source: HA→ Destination: MN** (CN_{PUK}).

Step 3: Send Message 3. In Message 3, the MN encrypts the MN's CoA and HoA using the CN's public key (the one sent by the CN to the MN via the HA). The encrypted message will be signed with the MN's private key that no one else has and sent directly to the CN.

- **Source: MN(CoA)→ Destination: CN**

$$\text{Sign}_{MN(PRK)}(\text{Enc}_{CN(PUK)}(\text{MN(CoA), MN(HoA)})).$$

Phase 3. In the last phase, the CN signature contained in the message is verified and checked for the correctness of the HoA. To authenticate the MN's signature, the CN will use the MN's public key, then decrypt the message and obtain the MN's CoA and HoA. The CN then calculates the hash of the HoA and compares it with the hash value from the first message. If either one of them receives a negative result, the message will be rejected. If the results of the checking operations and the validation process are positive, the CN is assured that the MN's HoA and CoA are correct. The CN will then send the binding acknowledgement (BA) to the MN.

V. Analysis of Private-Key-Based Binding Update Protocol

The BU message is vulnerable to different types of attacks, including the following: data packet interceptions that potentially allow attackers to eavesdrop on contents, thus violating the user's confidentiality or altering transmitted packets for the attacker's own malicious purposes; address spoofing attacks; and DoS or redirection attacks. This paper presents the proposed solutions to protect the BU message against these attacks. Our focus is on four major areas related to the security of the BU message: cryptography, authentication, ownership of the MN's HoA, and reachability of the MN at the CoA. Cryptography allows the transmitted data to be scrambled to render it undecipherable. In this way, intercepted packets are completely unreadable, and only those possessing the appropriate key can decrypt the data to make it readable. Authentication is the process of verifying the authenticity of the nodes involved in the communication process, while ownership and reachability involve checking the correctness of the MN's HoA and CoA. The exchange of messages between the MN and the CN provides strong evidence to the CN regarding the ownership of the MN's HoA. This is done using a one-way hash function to create IPv6 addresses along with the BU message that is signed using the MN own private key. In addition, in the proposed method, the hash value of the MN's HoA is sent in Message 1 to the CN through the HA. The MN then sends the HoA to the CN in Message 3, and the CN will calculate the HoA hash value and compare it with the hash value in Message 1 received via the HA. Thus, the reachability of the CoA has been checked. In the rest of this section, we present a simulated session hijacking attack, MITM attack, and DoS attack to evaluate the security requirements, ownership of the HoA, and reachability of the CoA.

Session hijacking attack. In the session hijacking attack, an attacker sends the CN a spoofed BU packet claiming to be the MN with the attacker's CoA. If the CN does not check the ownership of the HoA and the reachability of the CoA, it would create a binding for the MN's CoA and would subsequently send new data traffic to the attacker instead of to the MN. Data meant for the MN would not reach it, and all sensitive data (such as the CoA from the MN) will then be visible to the attacker if the message is not cryptographically secure (Fig. 11(a)). The proposed method can prevent this attack because an attacker does not have the MN's private key to sign the message containing the CoA. Also, the CN has to use the MN's public key to verify that the signature does not match the attacker's private key. If the authentication process fails, it means that the HoA and the CoA do not belong to the MN, which, in turn, means that the ownership and the reachability checks have failed, and the CN will not direct the data traffic to the attacker. As a result, the BU message will be protected against session hijacking attacks (Fig. 11(b)).

MITM attack. In an MITM attack, an attacker sends

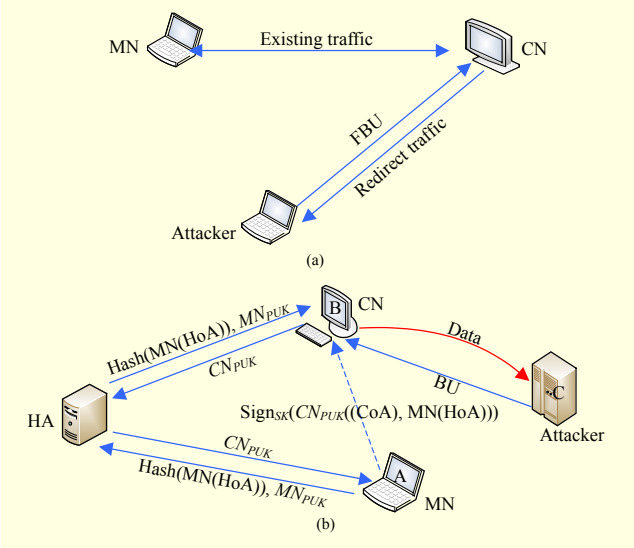

Fig. 11. (a) FBU attack and (b) FBU attack in PKBU.

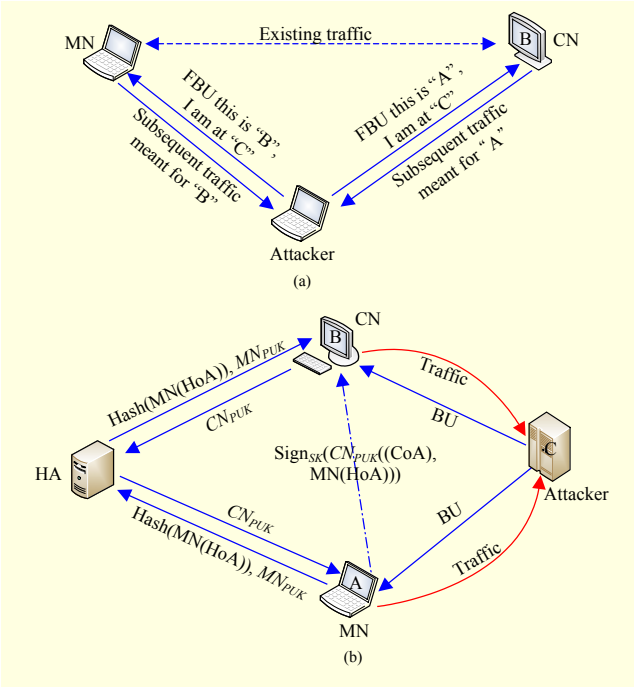

Fig. 12. (a) MITM attack and (b) MITM attack in PKBU.

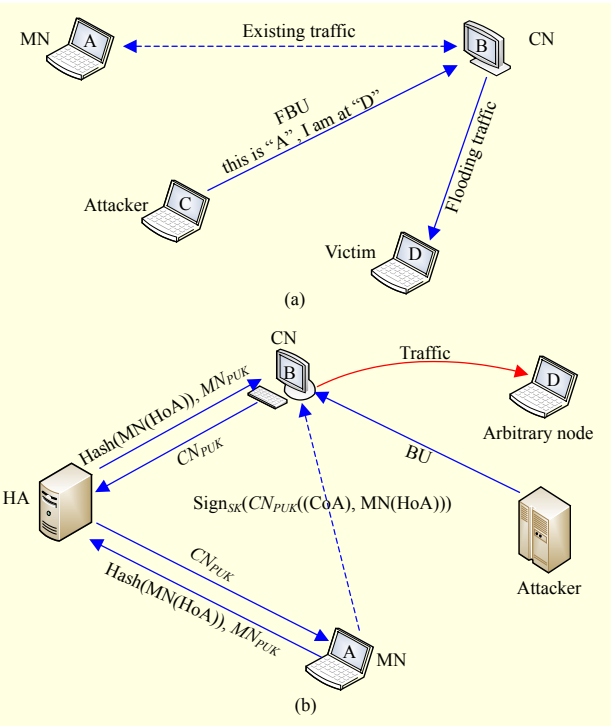

Fig. 13. (a) DoS attack and (b) DoS attack in PKBU.

spoofed BU messages to both the MN and the CN and also sets the CoA as its own address. As a result, the MN and the CN would both send the packets to the attacker instead of to each other, thus causing a breach in secrecy and integrity. This happens if the nodes do not check for ownership, reachability, and authenticity and merely accept the new CoA (Fig. 12(a)). This attack can be prevented by using the proposed method because of the node's signature, hash function, and cryptography algorithm. Figure 12(b) shows that if an attacker sends a BU message to the CN, the CN will check the ownership and the reachability of the IP addresses. In the proposed method, the ownership of the MN's IP address is checked by using the MN's private key to create a 128-bit IP address that is secure and cannot be spoofed by the attacker. In addition, the proposed method also checks the reachability of the IP address. To do this, the MN will send its HoA hash value to the CN via the HA, and the CN will then compute the HoA's hash value and compare it to the previous value. The attacker does not have the MN's private key to sign the message containing the CoA. Thus, by checking the authenticity, ownership, and reachability of the IP address, the CN can ensure that the BU message is from a valid MN and not from an attacker. An attack would only happen if the attacker has the MN's and the CN's private key. The proposed method makes it very difficult to get the node's private keys to mount an MITM attack. In addition, in an MITM attack, it is not possible for the attacker to eavesdrop on the users' message and compromise the user's confidentiality because the message is encrypted using cryptography algorithms.

DoS attack. In a DoS attack, spoofed BU messages are sent to create a lot of unnecessary data traffic to overwhelm the resources of a single node or a network node. The attacker would first identify a site with a heavy data stream (such as streaming video) to connect to. Then, it sends a BU to the CN, redirecting subsequent data traffic to a node by setting the victim's IP address as a CoA and its own address as an HoA. As a result, an excessive amount of redundant data traffic

would overwhelm the arbitrary node [33], [34]. Thus, if the CN is able to check the correctness of the HoA and CoA, then the CN can identify the BU, and it will not accept the CoA as a new IP address for the MN. As a result, the victim's node will not be flooded by a heavy stream of data (Fig. 13(a)) [35], [36]. The proposed method can also prevent DoS attacks. The CN will not accept a new CoA if a new message carries an unverified CoA. To verify the CoA, the CN must first verify the authenticity of the MN. The CN uses the MN's public key to verify the signature that is created based on the MN's private key. The signature cannot be verified if the attacker does not know the MN's private key that was generated based on the proposed method. The CN then checks the confidentiality of the message by decrypting the message using its own private key; subsequently, the CN can get the HoA and the CoA and check the ownership of the MN's HoA and the reachability of the CoA (Fig. 13(b)).

VI. Comparison of Existing Work with Proposed Method

The research presented herein concerns the security of BU messages between the MN and the CN. Table 2 shows the results of a comparison (based on authentication and integrity) between the proposed PKBU protocol and the current protocols, categorized as INF-less and INF-based [37]. Amongst the protocols included in Table 2 are hierarchical CBU (HCBU), shared key (SK), ticket-based BU (TBU), and password-based authenticated key exchange (PAK-based). We can conclude that the BU message can be protected in different ways and against different attacks, but the protection methods should be designed based on each case to minimize the iterating course within the entire protocol. This avoids redundancy in the protocol, thus improving efficiency as the

Table 2. Comparison results.

INF-less	Authenticate HoA	Authenticate CoA	Integrity of CoA	INF-based	Authenticate HoA	Authenticate CoA	Integrity of CoA
EBU	▲	▲	√	CBU	√	X	√
RR	▲	▲	√	HCBU	√	√	√
PBK	X	▲	√	SK	√	X	√
UDHBU	▲	X	√	TBU	√	X	√
OMIPv6	▲	X	√	PAK-based	√	▲	√
CGA-OMIPv6	▼	▲	√	▲ uses address reachability test ► uses CGA-based address ▼ uses CGA-based address and address reachability test			
ERO-MIPv6	▼	▲	√				
CAM	►	X	√				
PKBU	√	√	√				

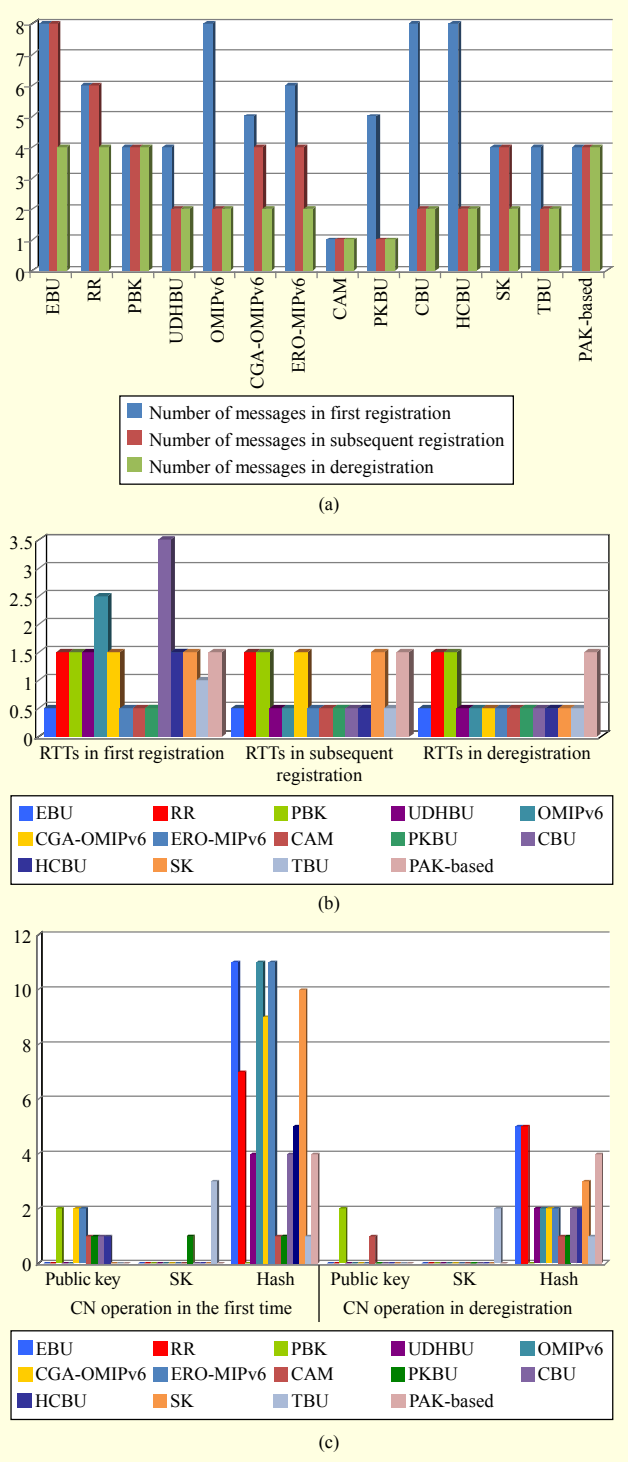

Fig. 14. (a) Number of messages, (b) RTT, and (c) operations.

iteration of course registration is reduced. The method must send BU messages in safe mode; otherwise, an attacker might succeed in attacking the nodes for its own malicious purpose. Figures 14(a) through 14(c) summarize the results of comparing PKBU to other protocols in regard to the following metrics: number of messages, round trip time (RTT), and operations.

VII. Conclusion

Many security solutions have been proposed for mobile communications. Each has its advantages and disadvantages. We reviewed the available protocols, and we discussed in detail the positive and negative aspects and the underlying design of these protocols to understand them better. The proposed protocol for BU authentication addresses the need to authenticate the mobile IPv6 location information [38]. When the MN and the CN send the control signal to each other via route optimization (RO), no shared secrets or trusted certificates exist during communication between the MN and the CN. Return routability (RR) is standardized to protect control messages in RO and to prevent third party attacks; However, RR can easily be broken, for example, if an attacker is able to intercept the RR messages. The PKBU protocol has low latency, which thus ensures faster handover, making it efficient in communication. This is because the protocol receives the necessary information even before the handover process is completed.

References

[1] C.E. Perkins, *Mobile IP: Design Principles and Practices*, Boston, MA, USA: Addison Wesley, 1998.

[2] J. Arkko, C. Perkins, and D. Johnson, "Mobility Support in IPv6," Internet Engineering Task Force, RFC 6275, July 2011.

[3] K. Ren et al., "Routing Optimization Security in Mobile IPv6," *Comput. Netw.*, vol. 50, no. 13, Sept. 15, 2006, pp. 2401-2419.

[4] A.S. Sadiq, K.A. Bakar, and K.Z. Ghafoor, "A Fuzzy Logic Approach for Reducing Handover Latency in Wireless Networks," *Netw. Protocols Algorithms*, vol. 2, no. 4, 2010, pp. 61-87.

[5] D. Johnson, C. Perkins, and J. Arkko, "IP Mobility Support," Internet Engineering Task Force, RFC 2002, Oct. 1996.

[6] S. Robert, "Introduction to Mobile IP," Institute for Information and Communication Technologies, Mar. 2003. http://www.stephan-robert.ch/attachments/File/Networking/MIP_sr_3_03- v2.pdf.

[7] M.A. Aydin, A.H. Zaim, and K.G. Ceylan, "A Hybrid Intrusion Detection System Design for Computer Network Security," *Comput. Electr. Eng.*, vol. 35, no. 3, May 2009, pp. 517-526.

[8] G. Martínez, F.G. Mármol, and J.M.A. Calero, "Introduction to Recent Advances in Security and Privacy in Distributed Communications," *Comput. Electr. Eng.*, vol. 38, no. 5, Sept. 2012, pp. 1033-1034.

[9] J. Arkko et al., "Secure Neighbor Discovery (SEND)," Internet Engineering Task Force, RFC 3971, Mar. 2005.

[10] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," Internet Engineering Task Force, RFC 3776, June 2004.

[11] K. Sahadevaiah and R.P.V.G.D. Prasad, "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks," *Netw. Protocols Algorithms*, vol. 3, no. 4, 2011, pp. 122-140.

[12] H. Soliman, *Securing Mobile IPv6 Signaling*, Boston, MA, USA: Addison-Wesley, 2004.

[13] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6)," Internet Engineering Task Force, RFC 2460, 2006, pp. 19.

[14] A. Conta and S. Deering, "Generic Packet Tunneling in IPv6," Internet Engineering Task Force, RFC 2473, 1998.

[15] O. Zuleger, "Mobile Internet Protocol v6," 2005. http://www.hznet.de/ipv6/mipv6-intro.pdf.

[16] P. Nikander et al., "Mobile IP Version 6 (MIPv6) Route Optimization Security Design," *IEEE Int. Conf. Veh. Technol.*, Orlando, FL, USA, vol. 3, Oct. 2003, pp. 2004-2008.

[17] K. Ren et al., "Routing Optimization Security in Mobile IPv6," *Comput. Netw.*, vol. 50, no. 13, Sept. 15, 2006, pp. 2401-2419.

[18] Z. Anari, *Security Enhancement of Route Optimization in Mobile IPv6 Network*, master's thesis, University of Putra Malaysia, 2008.

[19] O. Elshakankiry, *Securing Home and Correspondent Registrations in Mobile IPv6 Network*, doctoral dissertation, University of Manchester, UK, 2010.

[20] T. Aura, "Cryptographically Generated Addresses (CGA)," *6th Conf. Inf. Security*, vol. 2851, Bristol, UK, 2005, pp. 29-43.

[21] C. Vogt et. al., "Early Binding Updates for Mobile IPv6," *IEEE Wireless Commun. Netw. Conf.*, vol. 3, New Orleans, LA, USA, Mar. 13-14, 2005, pp. 1440-1445.

[22] F. Le and S.M. Faccin, "Dynamic Diffie Hellman Based Key Distribution for Mobile IPv6," Internet Engineering Task Force, Apr. 2001.

[23] R.H. Deng, J. Zhou, and F. Bao, "Defending Against Redirect Attacks in Mobile IP," *9th ACM Conf. Comput. Commun. Security*, New York, NY, USA, 2002, pp. 59-67.

[24] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," Internet Engineering Task Force, RFC 3775, June 2004.

[25] W. Haddad et al., "Optimizing Mobile IPv6 (OMIPv6)," Internet Engineering Task Force, Feb. 2004.

[26] W. Haddad et al., "Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6)," Internet Engineering Task Force, May 2005.

[27] J. Arkko, W. Haddad, and C. Vogt, "Enhanced Route

Optimization for Mobile IPv6," Internet Engineering Task Force, RFC 4866, May 2007.
[28] M. Roe et al., "Authentication of Mobile IPv6 Binding Updates and Acknowledgments," Internet Engineering Task Force, 2002.
[29] I. You, J.-H. Lee, and B. Kim, "caTBUA: Context-Aware Ticket-Based Binding Update Authentication Protocol for Trust-Enabled Mobile Networks," *Int. J. Commun. Syst.*, vol. 23, no. 11, Nov. 2010, pp. 1382-1404.
[30] H. Modares et al., "A Survey of Secure Protocols in Mobile IPv6," *J. Netw. Comput. Appl.*, available online Aug. 2013.
[31] G.M.D. Dormale, P. Bulens, and J.-J. Quisquater, "An Improved Montgomery Modular Inversion Targeted for Efficient Implementation on FPGA," *IEEE Int. Conf. Field-Programmable Technol.*, Brisbane, Australia, 2004, pp. 441-444.
[32] H. Modares et al., "A Bit-Serial Multiplier Architecture for Finite Fields over Galois Fields," *J. Comput. Sci.*, vol. 6, no. 11, 2010, pp. 1237-1246.
[33] J. Arkko et al., "Mobile IP Version 6 Route Optimization Security Design Background," Internet Engineering Task Force, RFC 2002, 2005.
[34] J. Arkko, C. Vogt, and T. Henderson, "End-Host Mobility and Multihoming with the Host Identity Protocol," Internet Engineering Task Force, Feb. 23, 2011.
[35] R.H. Deng, J. Zhou, and F. Bao, "Defending Against Redirect Attacks in Mobile IP," *Proc. 9th ACM Conf. Comput. Commun. Security*, Washington, DC, Nov. 18-22, 2002, pp. 59-67.
[36] T. Aura, M. Roe, and J. Arkko, "Security of Internet Location Management," *Proc. 18th IEEE Conf. Annual Comput. Security Appl.*, Las Vegas, NV, USA, Dec. 9-13, 2002, pp. 78-87.
[37] D. Kavitha and K.E.S. Murthy, S.Z. Hug "Security Analysis of Binding Update Protocols in Route Optimization of MIPv6," *Int. Conf. Recent Trends Inf., Telecommun. Comput.*, Kochi Kerala, Mar. 12-13, 2010, pp. 44-49.
[38] A. Datta et al., *Authentication for Mobile IPv6*, Department of Computer Science, University of Oxford, 2002, pp. 1-11. ftp://ftp.kestrel.edu/pub/papers/pavlovic/MIPv6.pdf.

Hero Modares is an assistant researcher in the Computer System & Technology Department, University of Malaya, Malaysia. She is currently a PhD student majoring in Mobile IPv6 security, Faculty of Computer Science and Information Technology, University of Malaya, and she obtained her MS from the same university in 2009. While earning her MS, she was a research assistant. Her research interests are in computer and network security, cryptographic protocol, digital signature and nonrepudiation, mobile communications security (MIPv6), and public-key infrastructure.

Amirhossein Moravejosharieh received his MS in the area of wireless networks from the University of Malaya, Kuala Lumpur, Malaysia. He is currently a PhD student in the field of wireless networks at the University of Canterbury, New Zealand. His primary area of research includes analyzing wireless networks in terms of handover procedures, QoS during handover procedures, and security issues related to handover procedures in Mobile IPv6 wireless networks.

Rosli Bin Salleh received his BS in computer science from the University of Malaya, Malaysia, in 1994, and his MS and PhD from the University of Salford, United Kingdom, in 1997 and 2001, respectively. From 2001, he worked as a lecturer in the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya. He was appointed as a senior lecturer in 2007 and as an associate professor in 2013. His research interests include Mobile IPv6 handover and security, botnet research, and wireless sensor networks.

Jaime Lloret received his MS in physics in 1997 from the University of Valencia and he finished a postgraduate MS in corporative networks and systems integration in the Department of Communications in 1999. In 2003, he received his MS in electronics engineering, University of Valencia. In 2006, he received his PhD in telecommunication engineering (Dr.-Ing.) from the Polytechnic University of Valencia. Before concluding his PhD thesis, he obtained the first place prize given by the Spanish Agency for Quality Assessment and Accreditation for the Campus of Excellence in the New Technologies and Applied Sciences Area. He was awarded the Best Doctoral Student in Telecommunications prize in 2006 by the Social Council of the Polytechnic University of Valencia. He has worked as a network designer and administrator for several companies. His academic interests and research include P2P networks, wireless local area networks, sensor networks, and routing protocols. He also conducts research on educational approaches and strategies.